HP Virus Throttle technology: stealth defense against malicious code in Microsoft® Windows® environments

technology brief

Abstract

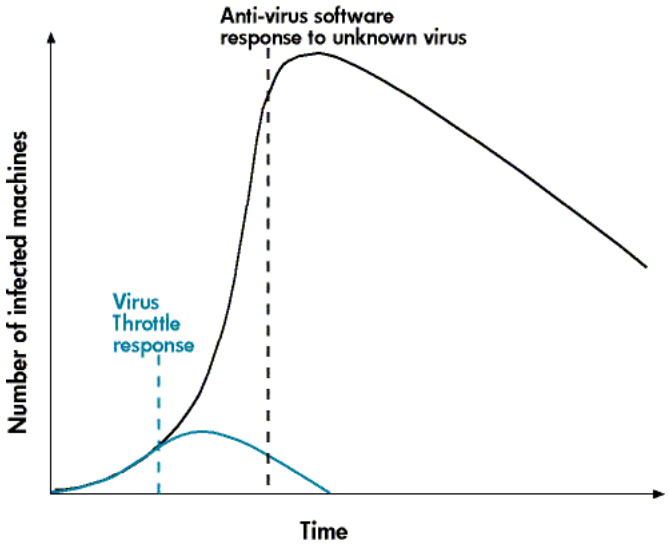
This paper describes how HP Virus Throttle technology works to mitigate the replication of fast-spreading worms and viruses that evade anti-virus software. Virus Throttle can detect and slow down the malicious code based on its behavior, giving IT personnel more time to respond to the infection. Virus Throttle represents a different paradigm in the battle against malicious code because it mitigates harm to other systems, rather than focus on the harm already done to an individual machine. Virus Throttle technology is available for servers running Microsoft® Windows® 2000 and Windows 2003 Server as part of the ProLiant Essentials Intelligent Networking Pack.

Introduction

Windows-based servers are under relentless attack from malicious computer viruses and worms. There are over 90,000 known viruses and worms with an estimated ten thousand more appearing annually. Anti-virus approaches are effective only against viruses with known signatures, which leaves most machines partially protected at best. When an infection occurs, the damage is not limited to individual machines; the network can become overwhelmed by the huge volume of traffic generated.

Virus Throttle technology is a different method for dealing with malicious code. If a previously unknown virus or worm infects a machine, Virus Throttle limits outgoing connections from that machine to greatly slow spread of the infection (Figure 1) and give administrators more time to respond. This also reduces the debilitating network traffic generated by fast-spreading malicious code. Virus Throttle works without virus signatures and, if it were widely deployed, would make network infrastructures resistant to known and unknown threats.

Figure 1. Faster response to virus attack lessens the impact (number of machines infected) by the infection



Characteristics of viruses and worms

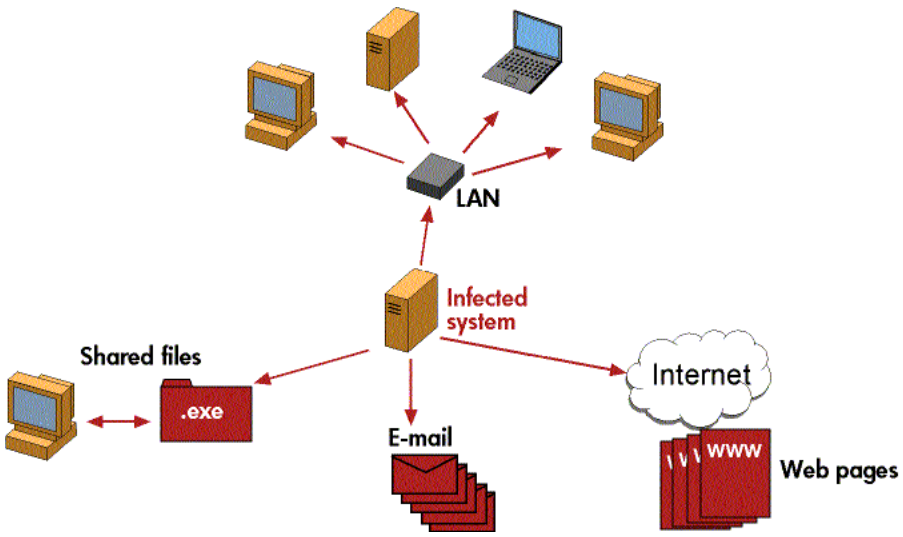
In general, a virus attempts to spread from computer to computer by attaching itself to a host program, which a user transmits by sharing or emailing the infected file. Worms, on the other hand, can scan networks and replicate themselves without user intervention. The main threat from worms and viruses is their ability to rapidly infect vast numbers of hosts. Once infected, these hosts can be used to launch massive denial of service attacks, steal or corrupt sensitive information, and disrupt the network with a flood of traffic.

How malicious code spreads in Windows environments

Fundamentally, a malicious code spreads when it can connect to vulnerable machines faster than humans or anti-virus software can respond. After malicious code infects one machine (Figure 2), it tries to infect other machines by one or more of the following methods:

- Infecting executable (.exe) files that may later be shared or requested by another user.
- Locating email addresses on the server and clients, and then mass mailing infected attachments.
- Taking over the web server process (possibly by using a buffer overflow technique) to launch further infection attempts.
- Propagating to file servers or other systems on the local area network (LAN).

Figure 2. Typical worm propagation



Virus and worm propagation have a major negative effect on network traffic. Under normal conditions, a machine makes a relatively low rate of connections to a short list of machines in any given second; a typical rate is about 1 connection per second (cps). In contrast, an infected system will make connection attempts to as many different machines as possible at an unusually high rate. One of the most infamous viruses, W32/Nimda-A (Nimda), used all of the methods described above to spread at an estimated rate of 400 cps. In January 2003, the W32/SQLSlam-A (SQLSlammer) worm infected almost 75,000 servers around the world in 30 minutes. The servers were running vulnerable versions of Microsoft SQL Server or MSDE 2000.

Limitations of signature-based anti-virus approaches

Current anti-virus approaches use signature-based detection methods to prevent *known* threats from entering a system. A signature, the virus' fingerprint, is a unique string of bits within the malicious code. Signature developers are skilled programmers who create a new signature for each virus or worm as it appears. Anti-virus software uses the virus signatures to scan for the presence of malicious code.

Signature-based anti-virus approaches have some limitations. First, signature development is fundamentally reactive with signatures being produced on a case-by-case basis. Secondly, developers can produce only a limited number of signatures in a given time; therefore, an unknown malicious code can spread unimpeded until the release of its signature. Thirdly, contemporary worms or viruses may have several variants. A form of virus known as polymorphic code poses a major threat because it mutates to remain undetectable to anti-virus software. Not all of the variants can be stopped by using a single signature.

Hackers constantly find minor and major vulnerabilities in software products, so IT administrators must be vigilant in installing patches and upgrades. If IT administrators do not apply patches consistently, a destructive worm can wreak havoc on an IT infrastructure. In the case of the SQLSlammer worm that struck in January 2003, Microsoft first made the patch available in July 2002, yet many IT administrators had not installed it. Even if administrators are diligent in installing patches, hackers have found another loophole. They are reverse-engineering patches to locate and exploit the vulnerability the patch was intended to fix.

Virus Throttle technology in HP ProLiant servers

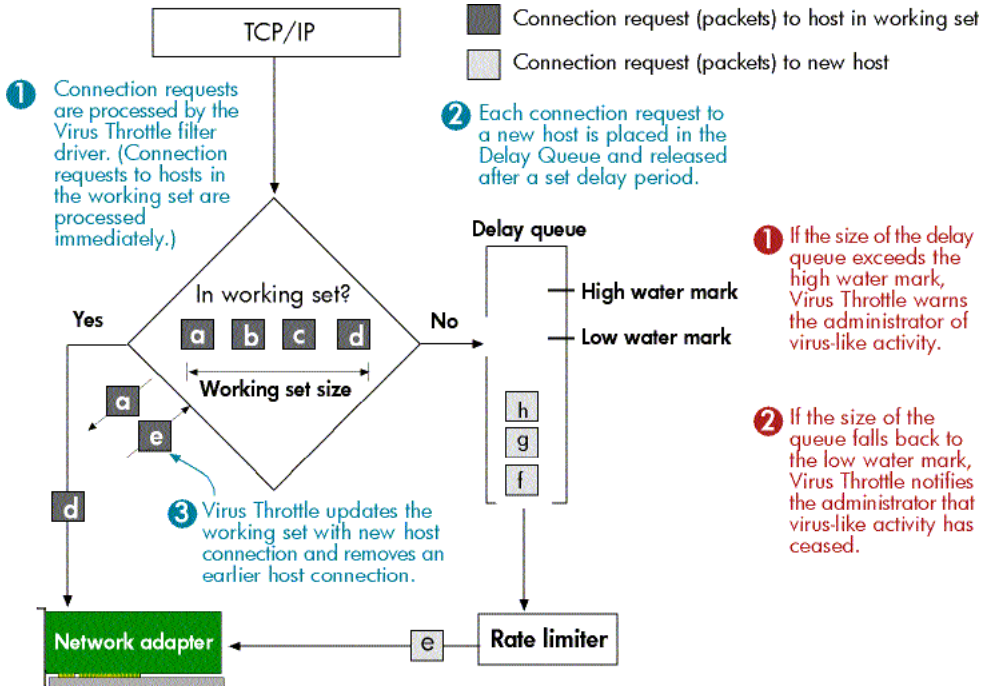
Virus Throttle technology is available as part of the ProLiant Essentials Intelligent Networking Pack (INP) for HP ProLiant servers running Microsoft Windows 2000 and Windows 2003 Server operating systems. Virus Throttle runs in the background and limits the outgoing connection rate to new systems based on parameters set by the administrator. If virus-like activity occurs, Virus Throttle will slow down the propagation and notify the IT administrator. Virus Throttle represents a new paradigm in anti-virus warfare: It does not need virus signatures to stop the spread of malicious code.

How Virus Throttle works

Virus Throttle technology limits the rate of TCP connections to new machines without interfering with the normal operation of the machine (Figure 3). When a connection request is made, Virus Throttle compares the destination host for the data packet to a working set (short list) of recently contacted hosts. If the destination host is listed in the working set, all packets to that host are processed immediately. If the destination host is not listed in the working set, the packets are sent to a delay queue. The packets in the delay queue are released and processed at regular intervals as determined by a rate limiter. The rate limiter guarantees that no more than one host address per time interval (set by the administrator) is processed. When a packet is processed to a new destination host, all other packets to the same host are processed.

If the frequency of requests to new hosts is higher than the pre-set frequency of the rate limiter, the size of the delay queue may rise to a pre-set threshold, or high water mark. If this occurs, Virus Throttle issues a WMI event to warn the administrator of virus-like activity. If ProLiant Insight Agents are installed on the system, an SNMP trap is also sent. If the size of delay queue drops below the low water mark, Virus Throttle issues a WMI event (and SNMP trap, if applicable) indicating that virus-like activity has stopped.

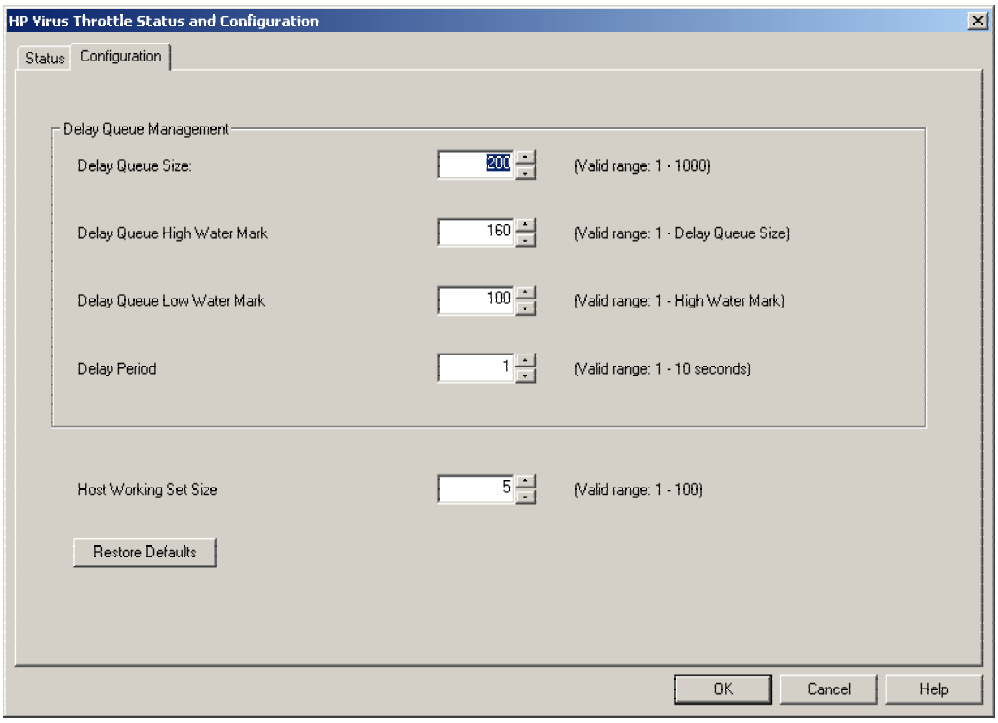
Figure 3. Virus throttling



Configuring HP Virus Throttle

Administrators control the sensitivity of Virus Throttle by configuring the settings in the user-friendly Windows GUI (Figure 4). These settings include the size of the delay queue, the low water mark, the high water mark, the size of the working set, and the delay period at which connection requests are released from the delay queue. Virus Throttle binds to all TCP protocol instances; therefore, a system with multiple network interface cards (NICs) will have multiple instances of Virus Throttle. The administrator configures the settings one time, and the settings apply to all instances of Virus Throttle.

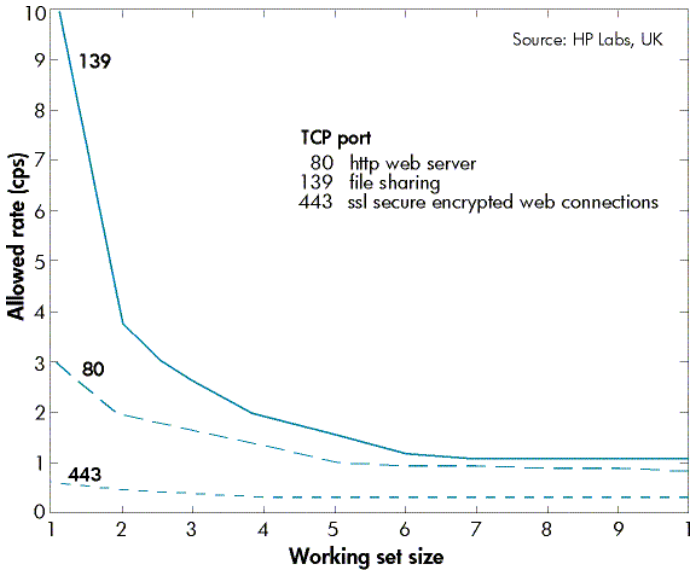
Figure 4. HP Virus Throttle Status and Configuration window in ProLiant Essentials INP



For a machine to be throttled effectively, its normal network traffic must not resemble virus-like activity—high outgoing connection rate and frequent connections to new hosts. Protocols that are conducive to virus throttling make repeated connections to the same hosts, for example, SMTP (port 25), IMAP (port 143), and web proxy (port 8088).

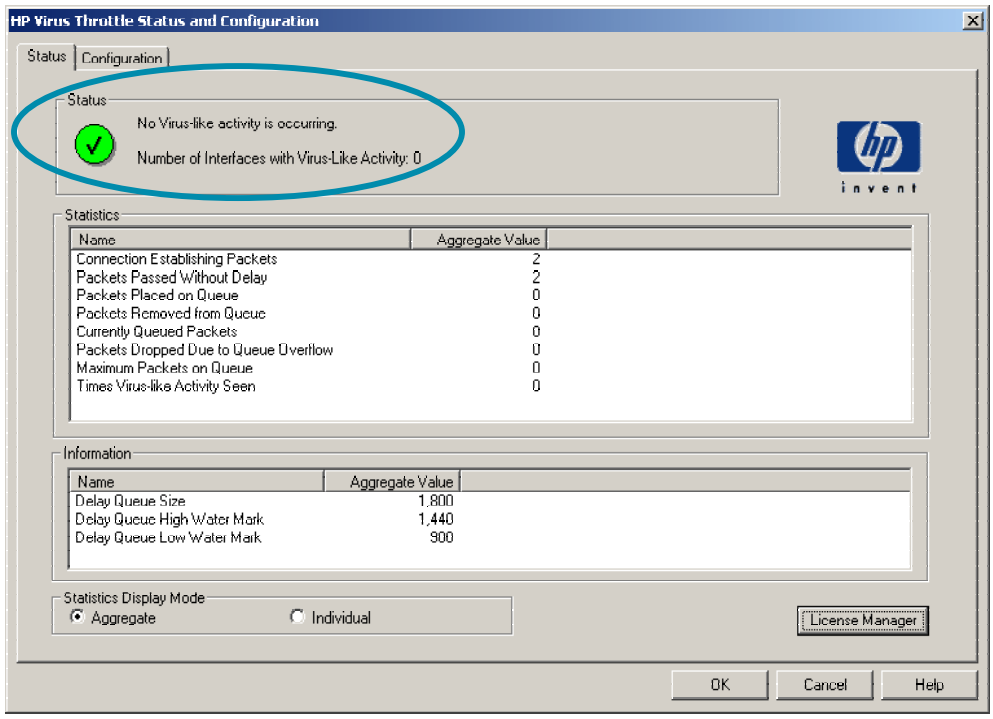
Some protocols for which the destination host changes can also be throttled if the configuration parameters do not result in the delay queue exceeding the high water mark for the typical range of network traffic. HP Labs conducted a test to simulate the effect of Virus Throttle settings for different protocols (Figure 5). The three lines on the graph correspond to network traffic with different destination ports. Test results showed that the best parameter settings are those with the smallest working set and lowest allowed rate, generally where each line begins to flatten out. For example, good parameter settings for http occur at a working set of 5 and an allowed rate of 1.

Figure 5. Throttle parameter settings for different TCP destination ports



By clicking the Status tab in the GUI (Figure 6), the administrator can view the statistics based on the configuration parameters. At the bottom of the window, the administrator can select Aggregate mode to view the statistics for all instances of Virus Throttle, or select Individual mode to view the statistics for separate instances.

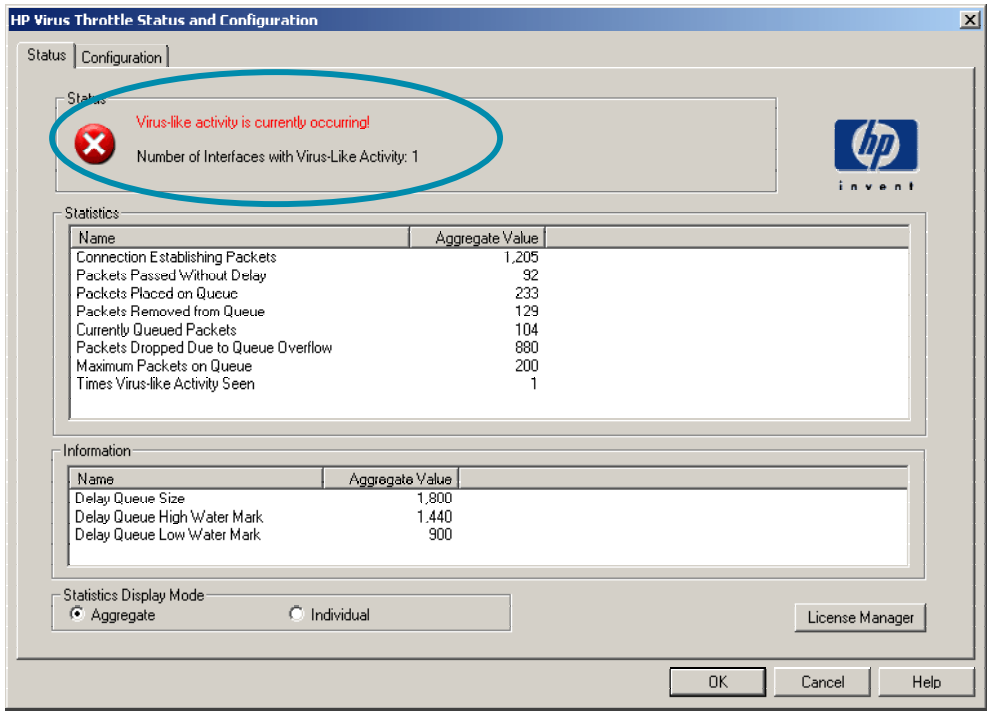
Figure 6. Virus Throttle statistics



Detecting virus-like activity

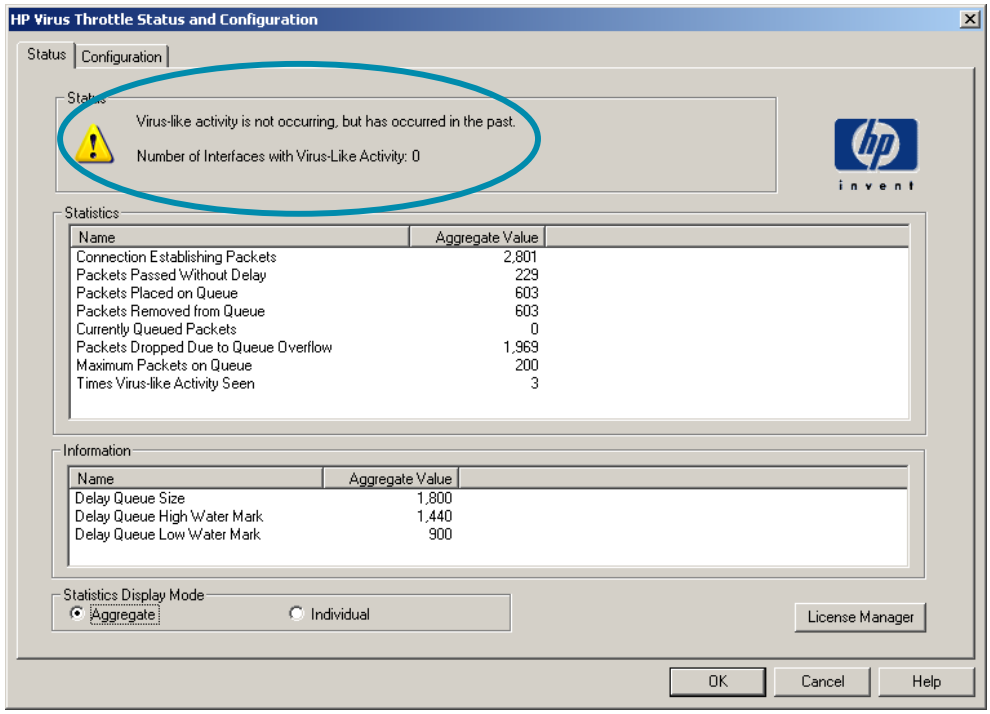
Virus-like activity is detected, and an alert is sent, when an individual Virus Throttle instance exceeds the delay queue high water mark. The activity continues until the size of the data queue falls below the low water mark. For example, Figure 7 shows that Virus Throttle is displaying a status message about virus-like activity because the number of currently queued packets (104) is between the low water mark setting (100) and high water mark setting (160) previously shown in Figure 4. Virus Throttle immediately notifies the administrator by issuing a WMI event. If ProLiant Insight Agents are installed on the system, an SNMP trap is also sent.

Figure 7. Notification of virus-like activity



If the number of currently queued packets falls below the low water mark, Virus Throttle displays the status message that virus-like activity has stopped (see Figure 8) and issues a WMI event (and SNMP trap, if ProLiant agents are installed) to the administrator.

Figure 8. Notification that virus-like activity has stopped



How fast is HP Virus Throttle?

Testing by HP Labs[1] showed that Virus Throttle is highly effective in detecting, slowing, and stopping real worms (Nimda and SQLSlammer in less than one second) and a test worm configured to scan at different rates (Table1). The test demonstrated that Virus Throttle can substantially reduce the global spread of a worm, and hence the amount of network traffic produced.

Table 1. Average time for Virus Throttle to stop real worms and a test worm scanning at different rates

Virus	Connections per second	Stopping time (seconds)	Connections made
Nimda	120	0.25	1
SQLSlammer	850	0.02	0
Test virus	2	106.00	104
Test virus	10	11.20	11
Test virus	60	1.40	1
Test virus	100	0.90	0
Test virus	200	0.02	0

[1] Proceedings 12th USENIX Security Symposium, 4-8th August 2003, Washington, DC, USA © Copyright Hewlett-Packard Company 2003

Conclusion

Virus Throttle technology is a different paradigm from signature-based anti-virus approaches in that it identifies malicious code based on its network behavior and, instead of preventing such programs from entering a system, seeks to prevent them from leaving.

Because Virus Throttle is triggered by the behavior of a virus, it can handle known and unknown threats without waiting for signature updates and patches. Virus Throttle allows the network infrastructure to stay up and running by slowing traffic from systems that exhibit high connection rates. Virus Throttle provides event log WMI events and SNMP trap warnings when worm-like behavior is detected. Most significantly, it gives IT staff time to react before the problem escalates to a crisis. If deployed widely, Virus Throttle makes it difficult for viruses to spread at all.

For more information

For additional information, refer to the resources detailed below.

Resource description	Web address
Virus Throttling white paper by HP Labs, UK	http://www.hpl.hp.com/techreports/2003/HPL-2003-69.pdf
Resilient Infrastructure for Network Security white paper from HP Labs, UK	http://www.hpl.hp.com/techreports/2002/HPL-2002-273.html
Implementing and testing a virus throttle white paper from HP Labs, UK	http://www.hpl.hp.com/techreports/2003/HPL-2003-103.pdf

TC050406TB/2005